Consulenza scientifica sul PIN delle carte di pagamento elettroniche a marchio BANCOMAT e PagoBANCOMAT

Consulenza scientifica sul PIN delle carte di pagamento elettroniche a marchio BANCOMAT e PagoBANCOMAT

Prof. Antonio Lioy
Politecnico di Torino
Dip. di Automatica e Informatica
(lioy@polito.it)

versione 1.0 (25/10/2013)

DOI: 10.6092/polito/porto/2539489

Indice

1 Oggetto della consulenza

Questo documento è stato scritto su richiesta del Consorzio Bancomat (nel seguito CB) per analizzare da un punto di vista scientifico la sicurezza logica e fisica della carte dei circuiti BANCOMAT e Pago-BANCOMAT. In particolare si vuole indagare se sia possibile l'uso fraudolento di una carta di pagamento (dotata di banda magnetica e chip) senza essere a conoscenza del PIN associato alla carta, con particolare riferimento ai seguenti punti:

- l'esistenza di possibili tecniche per pervenire alla clonabilità del chip e, ove esistessero, i tempi, i costi e le modalità con cui pervenire a tale risultato;
- le eventuali tecniche per estrarre il PIN dal chip e, ove esistessero, i tempi, i costi e le modalità con cui pervenire a tale risultato;
- le eventuali tecniche per pervenire all'utilizzo della carta a chip senza il ricorso al PIN e, ove esistessero, i tempi, i costi e le modalità con cui pervenire a tale risultato.

Le risposte qui fornite sono basate, al meglio delle conoscenze dell'autore, sulla documentazione esistente a giugno 2013 e fornita da:

- Consorzio Bancomat;
- società di servizi operanti per Consorzio Bancomat;
- fornitori delle carte o dei chip;
- società di gestione dei circuiti di pagamento;
- siti web Internet.

Infine si sottolinea che l'analisi qui svolta è esclusivamente relativa alle carte a marchio BANCOMAT e PagoBANCOMAT. Non sono state considerate le altre tipologie di circuiti di pagamento spesso associate a queste carte (es. FastPay, Maestro, Cirrus, Visa, MasterCard).

2 Le carte elettroniche di pagamento

2.1 Generalità

Le attuali carte elettroniche di pagamento sono supporti plastici dotati di una banda magnetica e/o di un dispositivo elettronico (*chip*, in italiano anche detto "microcircuito"), contenenti informazioni che permettono:

- il pagamento di beni o servizi, tramite dispositivi di tipo *POS (Point-Of-Sale)* come quelli installati nelle casse dei supermercati o presso esercizi commerciali (es. abbigliamento, ristorazione);
- il prelievo di denaro contante, tramite gli appositi dispositivi automatici *ATM (Automatic Teller Machine)*.

Collettivamente POS e ATM vengono solitamente identificati col nome di *terminale* perché costituiscono il punto dove termina il dialogo informatico col sistema di pagamento, essendo il punto in cui avviene un'interazione fisica con l'utente (introduzione della carta ed eventuale inserimento di un codice di sicurezza).

Le carte possono contenere diversi tipi di informazioni per l'uso in differenti *circuiti di pagamento*, ciascuno dei quali determina (per la parte di sua competenza) le informazioni memorizzate e le modalità d'uso della carta.

La coesistenza di diversi circuiti sulla stessa carta comporta necessariamente la definizione di *standard* per definire sia gli aspetti più semplici (es. la dimensione della carta, la posizione del chip) sia quelli più complessi ed importanti (es. la sicurezza dei dati e delle operazioni).

Per verificare che gli standard siano rispettati, esistono appositi laboratori che svolgono l'operazione di *certificazione* attraverso una serie di test.

Sono quindi di particolare rilevanza per il presente studio gli standard di sicurezza ed i relativi modelli di certificazione decisi a livello internazionale.

2.2 Confronto tra banda magnetica e chip

La tecnologia della banda magnetica permette di registrare informazioni sulla carta di pagamento scrivendole nell'apposita striscia plastica magnetizzata. La banda magnetica permette solo di memorizzare informazioni che possono essere lette e duplicate da chiunque entri in possesso – anche solo temporaneamente – della carta tramite un'apparecchiatura del costo di pochi Euro ed in un tempo brevissimo (meno di un minuto). Si tratta quindi di una tecnologia poco sicura perché permette facilmente di creare copie della carta, ossia di creare una carta clonata.

La tecnologia delle carte a chip consiste invece nel posizionare sulla carta un circuito elettronico integrato che può svolgere non solo funzioni di memoria ma anche elaborazioni, svolgendo cioè operazioni complesse. Per questo motivo sono anche dette *smart-card* perché, rispetto alle carte magnetiche, sono dotate di "intelligenza". In particolare i chip usati nelle carte di pagamento hanno il compito di memorizzare in modo sicuro le informazioni del titolare e di effettuare transazioni sicure verso i circuiti di pagamento associati alla carta. Come verrà chiarito meglio in seguito, la clonazione di una carta a chip è un'operazione difficile, lunga e costosa.

Si può quindi concludere che la tecnologia a chip è molto più sicura di quella a banda magnetica. La ragione per cui sono ancora in circolazione carte che contengono anche la banda magnetica, unitamente al chip, è da ricercarsi nella necessità di permettere l'uso della carta anche su terminali che supportano solo operazioni a banda magnetica. Questi terminali sono in via di completa dismissione in Italia ma hanno ancora una certa diffusione a livello mondiale.

2.3 Lo standard EMV

Nel campo delle carte di pagamento elettroniche a chip, lo standard *EMV* è quello universalmente riconosciuto come il più avanzato ed è universalmente accettato sia per le carte di debito sia per quelle di credito. Questo standard specifica sia il formato fisico del chip (e della carta che lo ospita) sia l'organizzazione del suo contenuto e l'interazione con le apparecchiature su cui può essere usato. EMV è nato nel 1993 dalla collaborazione dei principali circuiti di pagamento a livello mondiale (Europay, MasterCard e Visa, da cui il nome dello standard) per definire le specifiche che regolano le applicazioni di pagamento elettronico basate su carte a chip. Alle tre aziende fondatrici di EMV si sono poi aggiunti altri attori ed attualmente lo standard EMV è gestito da EMVco[1], organismo interamente posseduto in modo paritetico da American Express, JCB, MasterCard e Visa.

EMV dedica particolare attenzione alla sicurezza del chip e delle sue interazioni coi terminali: il secondo volume delle specifiche [1] è interamente dedicato a questo argomento ed esiste un apposito programma di approvazione e certificazione[2] sia per i terminali sia per i chip EMV. Esistono dieci laboratori altamente qualificati[3] riconosciuti dal consorzio EMV per condurre i test ed emettere le certificazioni di sicurezza. Questi laboratori applicano le tecniche di indagine più moderne e conducono prove relative a tutti gli attacchi noti alla data del test.

[1] http://www.emvco.com/
[2] http://www.emvco.com/approvals.aspx
[3] http://www.emvco.com/approvals.aspx?id=99

2.4 Svolgimento di una transazione a chip

Le carte di pagamento EMV possono operare in due modalità diverse. La prima vede l'esecuzione di transazioni on-line: in questo caso il terminale è connesso in rete al Centro Servizi, deputato ad autorizzare la transazione in tempo reale. La seconda consiste nell'esecuzione di transazioni off-line, nelle quali il terminale provvede esso stesso ad autorizzare la transazione e contatta il Centro Servizi solo successivamente.

Nell'ambito delle transazioni on-line, il Centro Servizi riceve un'informazione (Application Cryptogram, in breve *crittogramma*) che contiene i dettagli della transazione, cifrati con algoritmo 3DES con chiavi memorizzate in maniera sicura internamente alla carta. Il Centro Servizi verifica la bontà del crittogramma ricevuto ed invia un'analoga informazione alla carta, che a sua volta ne verifica l'autenticità, ai fini dell'autorizzazione finale dell'operazione di pagamento. La verifica del crittogramma consente di accertare l'autenticità della carta e la validità della transazione da parte del Centro Servizi e l'autenticità del Centro Servizi da parte della carta. La verifica positiva del crittogramma è fondamentale ai fini dell'autorizzazione finale dell'operazione di pagamento.

Nel caso di transazioni off-line, le informazioni relative alla transazione, opportunamente cifrate dalla carta, sono inviate in una fase successiva al Centro Servizi, permettendo – sia pure a posteriori – di verificare la bontà dell'operazione di pagamento.

Il Centro Servizi, per ogni transazione eseguita, registra nel proprio *log*[4] gli estremi della transazione, così che è sempre possibile sapere quali operazioni sono state effettuate con una certa carta, su quali terminali e con quali modalità.

Durante lo svolgimento di transazioni con tecnologia a chip, viene effettuato un ulteriore passaggio che attiene al riconoscimento dell'utilizzatore della carta che può essere realizzato attraverso diverse modalità definite all'emissione della carta (CVM, Cardholder Verification Method):

- l'introduzione di un codice numerico associato alla carta, detto PIN (Personal Identification Number);
- la firma autografa del titolare;
- nessuna verifica.

La verifica positiva del possessore della carta è fondamentale ai fini dell'autorizzazione finale dell'operazione di pagamento.

Solo successivamente alle verifiche finora descritte, ivi inclusa quella del titolare della carta di pagamento, l'operazione di pagamento viene effettivamente completata dal terminale.

2.5 Verifica del titolare

In merito alla verifica dell'utilizzatore della carta, l'identificazione tramite PIN risulta oggi il metodo più sicuro; esso infatti ricade nella categoria dei sistemi sicurezza detti "a due fattori" perché richiede sia il possesso della carta sia la conoscenza del PIN, che viene comunicato in modo sicuro al titolare della carta all'atto della sua consegna e di cui il titolare è obbligato a garantire la riservatezza.

La verifica del PIN può avvenire attraverso una delle seguenti modalità:

- PIN con verifica off-line, ossia il PIN viene scambiato nel colloquio tra terminale e carta e verificato dalla carta;
- PIN cifrato con verifica on-line, ossia il PIN viene trasmesso cifrato al Centro Servizi e verificato da quest'ultimo.

[4] Una sorta di registro informatico che tiene traccia delle operazioni svolte.

3 Il Consorzio Bancomat

Il Consorzio Bancomat è titolare dei marchi BANCOMAT e PagoBANCOMAT e, pur non emettendo direttamente carte di pagamento:

- definisce le regole per la gestione del circuito di pagamento (PagoBANCOMAT) e di quello di prelievo (BANCOMAT);
- definisce le regole per la diffusione e per l'utilizzo delle carte a marchio BANCOMAT e PagoBANCOMAT da parte degli aderenti ai circuiti;
- concede le licenze d'uso ai soggetti autorizzati alla gestione dei servizi di pagamento.

In generale le carte recano sia il marchio BANCOMAT, grazie al quale operano su ATM per il servizio di prelievo, sia il marchio PagoBANCOMAT grazie al quale eseguono operazioni di pagamento soprattutto su POS. Per completezza, si segnala che su alcuni ATM evoluti, il circuito PagoBANCOMAT può ugualmente essere usato per operazioni di pagamento (es. multe o bollette).

Nel seguito, per semplicità, si parlerà di "carte Bancomat" per indicare collettivamente le carte a marchio BANCOMAT e/o PagoBANCOMAT.

4 Le carte Bancomat

Attualmente le carte Bancomat sono tutte obbligatoriamente dotate di un chip secondo lo standard internazionale EMV. Molte di queste carte sono anche dotate di una banda magnetica, per permetterne l'uso anche sui pochi terminali che supportano solo operazioni a banda magnetica, o per compatibilità con altri circuiti di pagamento. Questo documento si concentra soprattutto sull'uso del chip e considera la banda magnetica solo marginalmente per spiegare come la sua presenza non modifichi il livello di sicurezza fornito dal chip.

Attualmente la totalità dei prelievi e la quasi totalità delle operazioni di pagamento effettuate con carte Bancomat avvengono con tecnologia a chip. Nei pochissimi casi in cui la transazione di pagamento avvenga con la lettura della banda magnetica, essendo tale operazione eseguita on-line, essa viene riconosciuta dal Centro Servizi, che valuta se concedere l'autorizzazione e, come per tutte le altre transazioni, ne registra lo svolgimento. E' quindi sempre possibile sapere se una determinata transazione è stata effettuata a chip o a banda magnetica.

Attualmente tutte le carte Bancomat operano in modalità on-line (ossia con un collegamento in rete al Centro Servizi, come descritto nella sezione 2.4), quindi i dati della transazione vengono verificati prima di concedere l'autorizzazione.

Attualmente tutte le carte Bancomat usano come metodo di verifica del possessore della carta l'introduzione del PIN associato alla carta nella modalità off-line (sezione 2.5).

Prima di essere emesse e consegnate al titolare le carte Bancomat seguono una procedura di omologazione che ne verifica la rispondenza agli standard internazionali ed alle direttive del Consorzio. In particolare una carta a chip deve essere dotata della certificazione internazionale EMV e poi subire una serie di ulteriori test che ne verificano la corrispondenza con le specifiche dei circuiti BANCOMAT e/o PagoBANCOMAT.

5 Primo quesito: clonabilità del chip

Per creare un clone di un chip occorre innanzitutto essere in possesso della carta (es. rubata, smarrita o sottratta temporaneamente) per cercare di leggere le informazioni memorizzate al suo interno e crearne quindi una copia.

In base allo standard EMV, non è possibile leggere tutte le informazioni contenute nel chip: alcune di queste (denominate "quantità segrete") vengono infatti usate dal chip per svolgere dei calcoli (generazione di "crittogrammi") il cui risultato è indispensabile per la validità della transazione di pagamento. Queste quantità segrete (tra cui è incluso anche il PIN del titolare) vengono usate dalla carta ma non sono estraibili tramite comandi di lettura perché il sistema operativo delle carte di pagamento non è stato dotato di tali comandi proprio per motivi di sicurezza (cfr. sezione A.3).

Avendo escluso un attacco diretto software, passiamo a considerare un attacco indiretto, ossia far svolgere alla carta delle operazioni per cercare di carpirne il contenuto in base ai risultati prodotti. Ad oggi l'unico attacco di questo tipo noto in ambiente scientifico è quello denominato di "power analysis" ossia l'osservazione della corrente elettrica assorbita dal chip durante il suo funzionamento. Questo attacco è stato analizzato nella sezione A.4, concludendo che i chip certificati sono resistenti a questo tipo di attacco dato che lo standard EMV richiede esplicitamente la protezione contro di esso.

Come terza ed ultima strada per cercare di leggere i dati contenuti nel chip si possono considerare attacchi hardware, ossia cercare di leggere fisicamente il contenuto del chip andando ad osservare la struttura dei suoi transistori. In linea di principio è possibile usare apparecchiature molto sofisticate (es. macchine per rimozione di sottili strati di materiale, microscopio elettronico a scansione) per rimuovere i contatti elettrici che coprono il chip e "leggere" i dati memorizzati al suo interno. Esistono ditte specializzate in grado di svolgere questo lavoro, ad esempio la MCU Engineering [2] offre questo servizio per fini leciti (analisi circuitale). Non si può quindi escludere che anche dei malintenzionati possano creare un laboratorio in grado di svolgere lo stesso lavoro effettuato da queste ditte. Si noti però che le apparecchiature necessarie sono molto costose (centinaia di migliaia di Euro), ingombranti (non sono apparecchiature portatili e richiedono anche l'uso di un laboratorio chimico molto ben attrezzato) ed il tempo necessario per l'operazione è variabile ma comunque molto lungo (da ore a giorni). Inoltre lo standard EMV richiede che i chip usati nelle carte di pagamento siano irrobustiti contro questi possibili attacchi hardware per complicarli o renderli impossibili (es. introducendo circuiti di auto-distruzione quando viene rimosso lo strato esterno) ed i laboratori di certificazione EMV adattano periodicamente i loro test alle nuove tecniche di attacco.

Si può quindi concludere che la clonazione di un chip non è possibile con procedure software mentre è possibile con un processo hardware ma esso richiede tempi e costi molto elevati, rendendo l'attacco più teorico che pratico: a meno che il titolare non si accorga del furto della carta, sicuramente la denuncia del furto (e quindi il blocco della carta) avverrà prima che gli attaccanti abbiano potuto duplicarne il chip.

6 Secondo quesito: estrazione del PIN

In virtù delle argomentazioni già condotte nelle sezioni precedenti è possibile affermare come non sia possibile estrarre il PIN da una carta Bancomat operando sul chip. D'altra parte, ancorché le carte siano dotate anche di una banda magnetica, va escluso che il PIN possa essere estrapolato da essa, in quanto la banda magnetica non contiene tale informazione (sul punto si veda la sezione A.2).

Gli unici modi ipotizzabili per venire a conoscenza del PIN associato ad una carta sono:

- l'intercettazione del PIN mentre viene trasmesso al verificatore per controllarne la correttezza;
- la lettura del PIN da un supporto su cui è stato conservato in modo insicuro dal titolare (es. un biglietto conservato insieme alla carta, un contatto nella rubrica di un cellulare rubato assieme alla carta).

Trascurando il secondo caso (perché non ha alcuna attinenza con la sicurezza delle carte ma riguarda invece il problema della corretta conservazione del PIN da parte del titolare della carta) vale la pena considerare qui l'altro caso.

L'intercettazione del PIN mentre viene introdotto sul terminale può essere effettuata manipolando il terminale (ad esempio sono state rinvenute in operazioni di polizia giudiziaria delle sovra-tastiere molto sottili che registrano i tasti premuti oppure delle micro-telecamere posizionate strategicamente per osservare il PIN introdotto).

Peraltro, l'acquisizione del PIN deve necessariamente essere seguita dal furto della carta altrimenti la conoscenza del PIN risulta inutile. Esaminando i log delle transazioni (presso il relativo Centro Servizi) è possibile sapere su quali terminali è stata usata la carta e quindi esaminarli per verificarne l'integrità o la manomissione.

Poiché per le carte Bancomat la correttezza del PIN viene sempre verificata dalla carta, esiste un'ulteriore possibilità di attacco quando il PIN viene introdotto tramite la tastiera del terminale e poi da questi trasmesso in chiaro alla carta tramite i suoi contatti elettrici. E' quindi possibile manomettere il POS introducendo al suo interno una sottile lamina (detta "shim") che va a coprire i contatti della carta e registra le informazioni scambiate tra essa ed il POS. E' così possibile leggere il PIN mentre viene trasmesso alla carta per verifica. Anche in questo caso l'acquisizione del PIN deve poi essere seguita dal furto della carta altrimenti la conoscenza del PIN risulta inutile. Inoltre in caso di operazioni sospette è possibile controllare i POS su cui sono state svolte le ultime transazioni di una carta per verificare che non contengano uno shim.

Appare quindi evidente come nei casi appena considerati non si realizzi alcuna estrazione del PIN dalla carta. A realizzarsi è invece l'intercettazione del PIN mentre viene introdotto dal titolare attraverso varie tecniche che però presuppongono tutte manomissione del terminale (o dell'ambiente in cui è posizionato).

L'analisi dei log delle transazioni può permettere di identificare i terminali manomessi e quindi di individuare gli eventi che effettivamente derivano da manomissioni.

7 Terzo quesito: uso della carta a chip senza l'uso del PIN

In linea di principio una carta a chip non può essere usata senza la corretta digitazione del PIN.

Sono noti in letteratura (e per completezza sono discussi in appendice) alcuni attacchi molto sofisticati ma di difficile esecuzione.

L'attacco "Null PIN" (sezione A.5) non è possibile contro le carte Bancomat perché tutte le transazioni sono svolte on-line e tra i dati proprietari trasmessi in modo sicuro dalla carta è inclusa anche la modalità di verifica del titolare. Nel caso che il PIN non sia stato inserito (come nell'attacco Null PIN) la transazione verrebbe rifiutata dal Centro Servizi.

L'attacco "pre-play" (sezione A.6) prevede di modificare un terminale per far pre-generare alla carta una serie di transazioni future. Affinché tali transazioni possano essere eseguite nel futuro è indispensabile che siano svolte sul terminale manomesso e soprattutto che la carta sia ancora valida (perché altrimenti il Centro Servizi non accetterebbe la transazione) e quindi non si applica a carte di cui sia stato denunciato il furto o smarrimento e di cui si ipotizza l'uso senza conoscerne il PIN. Inoltre al primo uso della carta originale si genererebbe un disallineamento nei contatori applicativi rispetto alla carta simulata dal terminale manomesso. Poiché tutte le transazioni con carte Bancomat sono svolte on-line, questo disallineamento verrebbe notato dal Centro Servizi che perciò rifiuterebbe la transazione. Infine, sempre per via del fatto che le transazioni con carte Bancomat sono svolte on-line, poiché le transazioni pregenerate non contengono l'indicazione circa l'avvenuta verifica del PIN, essere verrebbero tutte rifiutate dal Centro Servizi.

Si può quindi concludere che l'uso di una carta Bancomat a chip senza conoscerne il PIN non è possibile.

8 Conclusioni

Al termine dell'analisi svolta posso così riassumere i risultati raggiunti.

Data una carta Bancomat smarrita o rubata non è possibile con tempo e risorse limitate riuscire ad estrarre da essa il PIN contenuto nel chip. L'operazione è teoricamente possibile ma richiede un laboratorio molto sofisticato (chimico ed elettronico) e quindi ha un costo molto elevato (centinaia di migliaia di Euro) e richiede comunque tempi molto lunghi (parecchie ore o giorni), incompatibili col riuso della carta prima della denuncia di perdita della stessa da parte del titolare. Ne consegue che una carta a chip non può essere usata senza conoscerne anche il PIN. Lo stesso tipo di laboratorio (e quindi gli stessi tempi e costi) è necessario nel caso si cerchi di clonare una carta a chip.

E' possibile conoscere il PIN associato ad una carta manomettendo un terminale per "catturare" il PIN durante la sua introduzione (es. tramite una sovra-tastiera o uno *shim*) oppure osservando con una micro-telecamera l'introduzione del PIN. E' però poi necessario il furto della carta ed in ogni caso è possibile verificare l'effettiva manomissione dei terminali su cui è stata usata la carta prima di una transazione sospetta o disconosciuta.

In letteratura sono noti alcuni attacchi che permettono di usare una carta rubata senza conoscerne il PIN (attacco Null PIN) oppure pre-generare una serie di codici autorizzativi durante un normale pagamento su un POS manomesso e quindi farli trasmettere da una carta fasulla (attacco pre-play). Come discusso in precedenza, questi due attacchi hanno una valenza più teorica che pratica e quindi l'uso di una carta Bancomat a chip senza conoscerne il PIN è nella pratica impossibile.

A Analisi tecnica di vari attacchi

Questa appendice contiene un'analisi più tecnica di vari attacchi, alcuni menzionati nelle sezioni principali di questo documento, altri qui esaminati per completezza perché hanno avuto una certa eco mediatica.

A.1 Clonazione della banda magnetica

La banda magnetica delle carte di pagamento è facilmente leggibile con apparecchiature del costo di poche decine di Euro ed in pochi secondi. Poiché le informazioni registrate sulla banda magnetica non sono protette in alcun modo (ossia non sono crittografate), ne consegue che chiunque entri in possesso (anche temporaneamente) della carta può fare una copia della sua banda magnetica su un'altra carta.

In questo modo è possibile clonare la parte magnetica della carta (ma non il chip!) e ne sarà possibile l'uso solamente in quei casi in cui il terminale legge la banda magnetica e non verifica l'identità tramite l'introduzione del PIN. Poiché la quasi totalità delle transazioni con carte Bancomat avviene tramite lettura del chip più introduzione del PIN, la clonazione della banda magnetica non ha rilevanza pratica per queste transazioni. Nel caso che la transazione sia condotta a banda, la differenza viene annotata nei log ed è quindi sempre possibile sapere se una specifica transazione è stata fatta a banda magnetica o chip (ed in ogni caso occorre conoscere anche il PIN associato alla carta).

Si può concludere che – nonostante sia facile copiare e duplicare la banda magnetica di una carta – la clonazione della banda magnetica non costituisce una minaccia per le transazioni a chip.

A.2 Recupero PIN dalla banda magnetica

La banda magnetica delle carte Bancomat è organizzata in tracce. I circuiti BANCOMAT e PagoBANCOMAT usano la traccia numero 3, su cui sono registrate una serie di informazioni che identificano univocamente il rapporto bancario del titolare della carta:

- codice ABI (Associazione Bancaria Italiana), 5 caratteri usati per identificare l'istituto finanziario che ha emesso la carta;
- codice diversificazione carta (1 carattere);
- codice PAN (Primary Account Number), codice identificativo univoco della carta composto da 11 caratteri;
- codice CIN (Control Internal Number) codice di controllo calcolato su ABI e PAN, composto da un solo 1 carattere.

Si noti che la banda magnetica è leggibile (con un apposito lettore) da chiunque entri in possesso della carta ma non contiene in alcuna forma il PIN associato alla carta.

Si può concludere che – nonostante sia facile copiare e duplicare la banda magnetica di una carta – non è possibile in alcun modo estrarre dalla banda stessa il PIN, perché esso non è presente tra i dati registrati nella banda magnetica.

A.3 Recupero PIN dal chip tramite tecniche software

Il chip presente sulle carte Bancomat è conforme allo standard EMV. Alle carte Bancomat è sempre associato un PIN memorizzato sul chip stesso in un'area proprietaria e protetta, come documentato nella specifica del Consorzio Bancomat [3], sezione 7.3.2.1.

value	level	presence	format
MAC DEA Key A	Application	Mandatory	b 64
MAC DEA Key B	Application	Mandatory	b 64
PIN DEA Key A	Application	Mandatory	b 64
PIN DEA Key B	Application	Mandatory	b 64
Unique DEA Key A	Application	Mandatory	b 64
Unique DEA Key B	Application	Mandatory	b 64
PIN Try Limit	Application	Mandatory	b 8
Reference PIN	Application	Mandatory	cn 4-12
ICC Private Key	Application	Optional	80-248

Figura 1: La Tabella 15 del documento [3].

> *7.3.2.1 Application Level Secret Data*
> *The data elements listed in Table 15 shall be stored securely within the card in one or more proprietary files. These data elements shall never be retrievable by a terminal or any outside source. Other than the Reference PIN, which may be updated using secure issuer scripts, the data in Table 15 shall never be updated.*

La tabella 15 (Fig. 1) della specifica citata elenca tra i dati segreti l'elemento *Reference PIN* che è il PIN associato al chip.

Si noti che la specifica richiede che i dati segreti non siano leggibili dall'esterno: infatti tutti i comandi relativi al PIN ne permettono solo la verifica (controllo che il PIN introdotto da tastiera sia uguale a quello memorizzato sulla carta) oppure l'aggiornamento (sovrascrittura con un nuovo PIN). In nessun caso è possibile tramite un comando leggere nessuno dei dati segreti elencati nella tabella 15 della specifica.

Si conclude che non è possibile impartire comandi al chip per comunicare il PIN al richiedente (ossia "estrarre" il PIN dal chip tramite un apposito software).

A.4 Attacco al chip tramite "power analysis"

Come descritto nella sezione 2.4, per ogni transazione la carta genera un crittogramma che viene usato dal Centro Servizi per autenticare la transazione stessa. Il crittogramma viene generato mediante cifratura di dati specifici della transazione, tramite algoritmo 3DES ed utilizzo di chiavi crittografiche uniche per ogni carta e memorizzate sul chip all'emissione.

Se il chip non è dotato di speciali protezioni allora è possibile effettuare uno dei vari attacchi della famiglia *Power Analysis* [4]: *SPA (Simple Power Analysis)*, *D*PA (Differential Power Analysis), e *HO-DPA (High-Order Differential Power Analysis)*. In pratica, osservando la corrente assorbita dalla carta durante un'operazione crittografica, è possibile capire quali sono i bit che costituiscono la chiave crittografica usata nell'operazione. I tre metodi SPA, DPA e HO-DPA si differenziano solo per il loro grado di crescente sofisticazione e quindi per la difficoltà nel creare un chip in grado di resistergli. Questa famiglia di attacchi è nota dal 1998 ed i produttori di chip crittografici hanno sviluppato varie contromisure (richieste anche da alcuni standard, ad esempio il FIPS 140-3 ed indirettamente anche da EMV). Si noti che questo campo è in continua evoluzione e vengo scoperte nuove tecniche che vanificano le protezioni messe in atto sui chip in circolazione. Ad esempio, tramite l'uso delle *wavelet* [5] nel 2005 è stato possibile superare le difese create contro gli attacchi SPA e DPA.

Le carte del Consorzio Bancomat sono certificate dai produttori del chip contro tutti gli attacchi di questa tipologia noti alla data di produzione del chip. Il Consorzio Bancomat omologa solo carte che dispongano delle certificazioni di sicurezza MasterCard (CAST) e Visa. La verifica di ottenimento di tali certificazioni è effettuata nel corso delle attività di omologazione da parte del personale del Consorzio

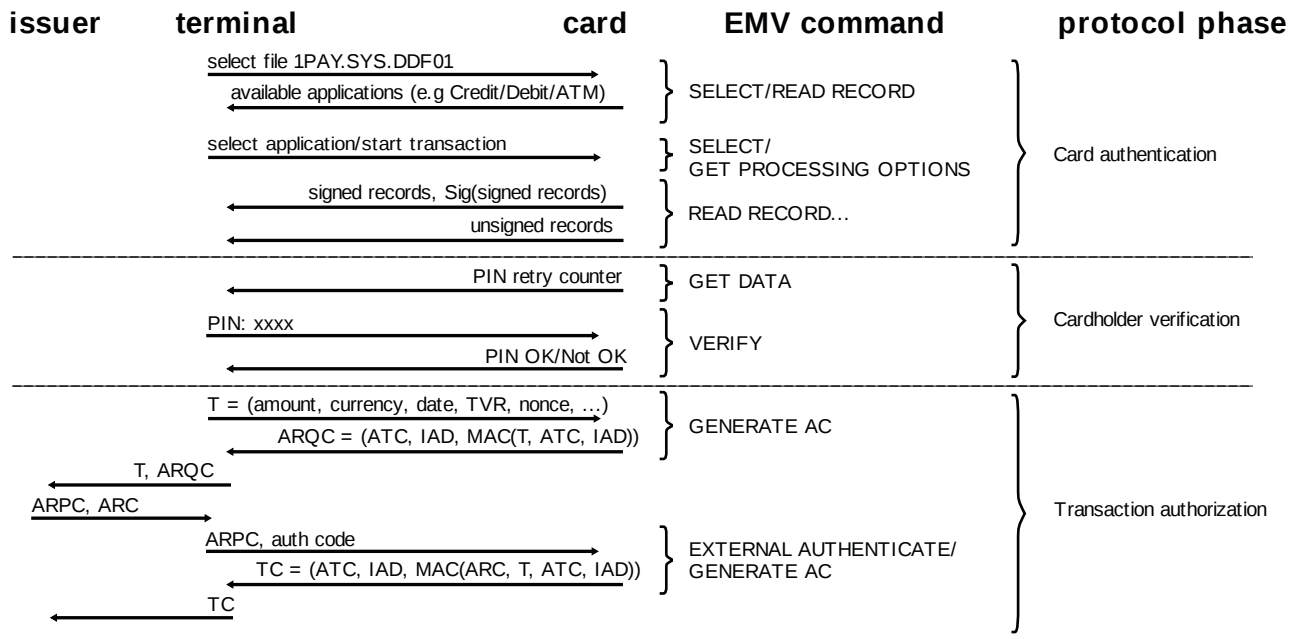

Figura 2: Schema dell'interazione carta-terminale in un pagamento EMV chip più PIN.

Bancomat. Le certificazioni e le omologhe hanno una durata temporale limitata[5] proprio per permettere di verificare la resistenza dei chip ad eventuali nuovi attacchi emersi durante il lasso di tempo trascorso dalla precedente certificazione.

Si può quindi concludere che gli attacchi di power analysis non pongono alcun pericolo all'operatività delle carte Bancomat.

A.5 L'attacco "Null PIN"

Alcuni ricercatori dell'Università di Cambridge hanno ideato un attacco che sfrutta un'opzione nel protocollo EMV, dimostrando sperimentalmente che tale attacco permette di fare operazioni su un POS con una carta rubata di cui non si conosce il PIN [6].

L'attacco è possibile perché la fase di verifica del PIN non è autenticata esplicitamente, ossia la risposta Pin OK non è accompagnata da un MAC (Fig. 2). Inoltre i dati autenticati inviati dal POS alla banca comprendono TVR[6] e IAD[7] ma il TVR fornisce un'indicazione generica di "verifica OK" senza indicare quale specifico metodo è stato usato per la verifica.

E' quindi possibile costruire un'apparecchiatura che funga da *MITM (Man-In-The-Middle)* tra la carta ed il terminale e risponda sempre in modo positivo (ossia con risposta 0x9000) qualunque sia il PIN introdotto sulla tastiera del terminale. In pratica la carta crederà che il terminale non supporti la verifica del PIN (visto che non riceverà il relativo comando) oppure che abbia scelto di autenticare il titolare tramite una firma autografa. A sua volta il terminale crederà che la verifica del PIN abbia avuto successo visto che ha ricevuto una risposta positiva.

Si noti che lo IAD talvolta indica il metodo usato per effettuare la verifica del titolare. Purtroppo il contenuto della IAD non è specificato nello standard EMV ed è quindi specifico delle varie applicazioni. Ne consegue che il terminale (che conosce il CVM usato) non può verificare se è riportato correttamente nello IAD.

I ricercatori di Cambridge hanno realizzato quest'attacco creando una smart-card falsa (da introdurre nel terminale) collegata tramite una *piattina* alla carta da attaccare (quella ipoteticamente rubata). Il loro

[5] Le omologazioni del Consorzio Bancomat hanno una validità massima di due anni.
[6] TVR = Terminal Verification Results, il risultato delle verifiche svolte dal terminale e dalla carta.
[7] IAD = Issuer Application Data, dati specifici di ogni emettitore di carte.

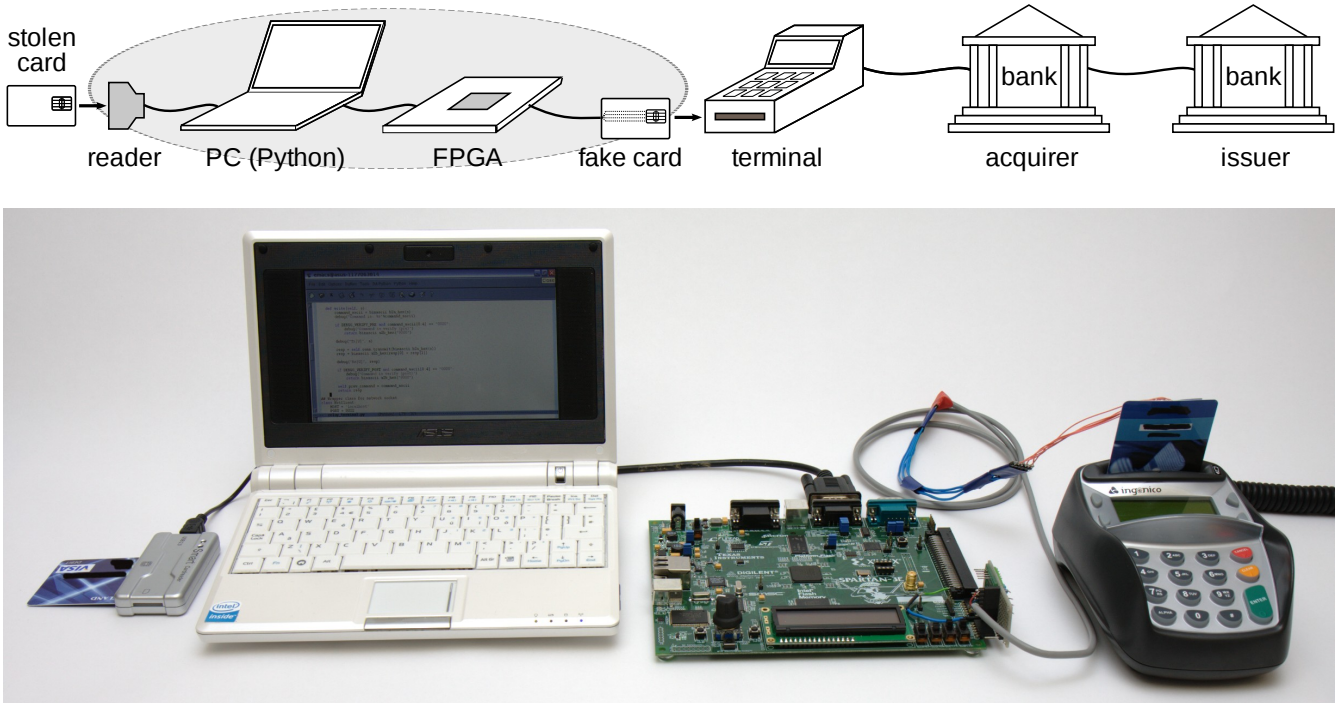

Figura 3: Setup sperimentale dell'attacco MITM dell'Università di Cambridge [6].

impianto sperimentale è voluminoso (Fig. 3) ma i ricercatori dichiarano che con una spesa non superiore a 1000 Euro è possibile ridurlo ad un oggetto delle dimensioni di un cellulare in cui inserire la carta e da portare in una tasca della giacca, facendo uscire la piattina di collegamento da una manica. Occorre una certa di destrezza nel tenere in mano la carta falsa per non far notare al negoziante la piattina di collegamento (che fuoriesce dalla parte inferiore della carta falsa). Potenzialmente più facile sarebbe l'uso su terminali POS non sorvegliati, come quelli diffusi in molti supermercati per il pagamento senza cassiera. Infine – date le capacità di miniaturizzazione evidenziate dai malviventi in recenti attacchi (il cosiddetto caso "foglia d'oro") – è anche possibile ipotizzare la costruzione di un mini-dispositivo (anche detto *shim*) da applicare sopra ai contatti del chip rendendolo solo un poco più spesso del normale ma la produzione di un simile tipo di dispositivo non è ancora nota.

E' interessante notare come gli scontrini generati dal POS in questo attacco (Fig.4) riportino la dicitura "Verified by PIN" nonostante la verifica del PIN non sia stata effettuata (!). Questo attacco ha avuto una notevole risonanza nel Regno Unito perché la BBC ha realizzato un servizio in cui si vede lo svolgimento dell'attacco [7]. Si noti che l'attacco è possibile solo su terminali POS che effettuano la verifica off-line del PIN.

Vale la pena menzionare che il software necessario per effettuare questo attacco (ma anche per svolgere generici test del protocollo EMV) è liberamente disponibile su Internet [8, 9] mentre il corrispondente hardware è in vendita per 480 GBP [10].

Come nota finale, si osserva che l'attacco Null PIN non è solo teorico ma reale; infatti esso è stato effettivamente realizzato in Francia, ma gli autori sono stati catturati e processati [11].

Passando però dal caso di generiche carte EMV (quelle usate in Gran Bretagna e studiate dai ricercatori di Cambridge) all'oggetto della consulenza, l'analisi svolta ha permesso di evidenziare che l'attacco Null PIN non si applica alle carte Bancomat perché la specifica del Consorzio Bancomat ([3] sezione 8.5.1) richiede che tra i dati inseriti nel pacchetto IAD sia presente il metodo usato per la verifica dell'identità del titolare. Siccome tutte le transazioni Bancomat avvengono on-line, il Centro Servizi può verificare se il PIN è stato introdotto e verificato dalla carta (caso normale) oppure il PIN non è stato introdotto (caso dell'attacco Null PIN). Nel secondo caso la transazione non verrà autorizzata e sarà generato un allarme.

Si può quindi concludere che l'attacco Null PIN non è possibile nei confronti delle carte Bancomat.

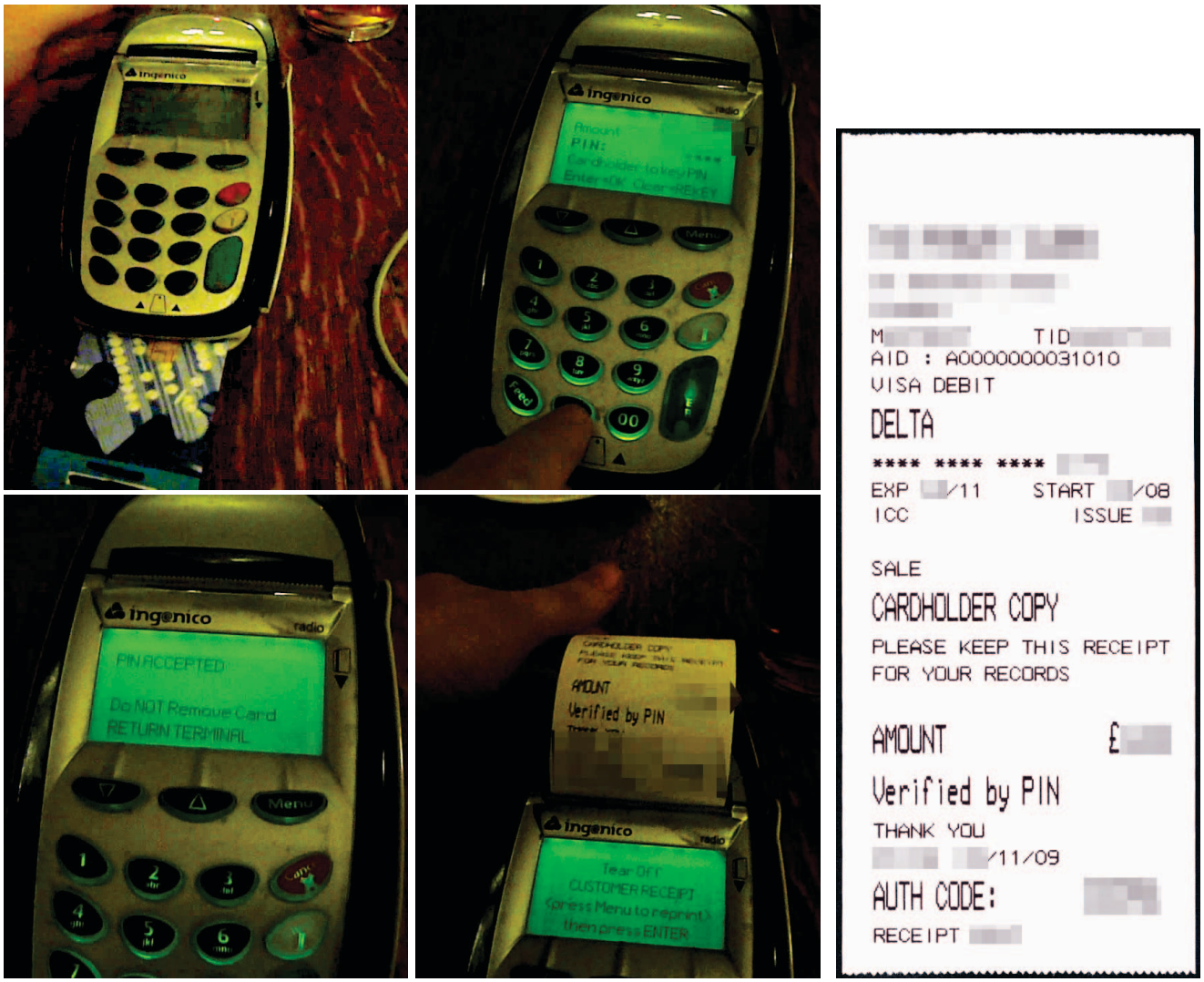

Figura 4: Immagini dell'attacco MITM e degli scontrini generati dal POS [6].

A.6 L'attacco pre-play (pseudo-clonazione di carte EMV)

Ricercatori dell'Università di Cambridge hanno identificato nel 2012 un attacco (detto "pre-play") che permette di effettuare transazioni valide indistinguibili da quelle che si potrebbero ottenere con una carta EMV clonata [12]. Questa analisi è stata usata in giudizio a supporto di un utente maltese che contestava a HSBC vari prelievi fatti apparentemente con la sua carta.

L'attacco si basa sulla predicibilità di un parametro della transazione EMV, il cosiddetto *Unique Number (UN)*, generato in maniera univoca dal terminale per ogni nuova transazione ed inviato alla carta per il calcolo del crittogramma. In pratica, si manomette un terminale (tipicamente un POS ma è possibile anche con un ATM) per fargli richiedere alla carta di generare tanti crittogrammi per autorizzare transazioni future con vari UN. Il numero di crittogrammi generabili è limitato dalla durata massima di una transazione: per una transazione di 30 secondi si riescono a collezionare circa 100 crittogrammi. Ciascun crittogramma corrisponde ad uno specifico valore (futuro) di UN. A questo punto si crea una smart-card fasulla che contenga – oltre al normale chip – anche un piccolo dispositivo per fare il "replay" di uno dei crittogrammi pre-generati quando vede che il terminale richiede uno degli UN previsti.

Questo attacco è fattibile ma bisogna prefissare alcuni parametri:

- il paese ove si userà la carta contraffatta;
- la data in cui si svolgerà l'operazione;
- l'importo dell'operazione fraudolenta.

Inoltre i crittogrammi pre-generati possono essere inviati solo dal terminale che è stato manomesso, il che facilita l'individuazione dello stesso e quindi delle operazioni fasulle.

Nel caso delle carte Bancomat, ci sono una serie di fattori che limitano ulteriormente l'applicabilità di questo attacco.

Innanzitutto occorre che la carta rimanga valida per un certo periodo nel futuro e quindi non si applica al caso di carte rubate o smarrite, di cui il titolare denunci tempestivamente la perdita.

Inoltre poiché tutte le transazioni sono svolte on-line e tra i dati applicativi scambiati ci sono anche dei valori numerici (contatori) che indicano il numero di operazioni svolte con la carta, al primo uso di una tra la carta originale e quella fasulla si creerebbe un disallineamento che verrebbe notato dal Centro Servizi impedendo le successive transazioni.

Ma soprattutto ciò che impedisce l'esecuzione di questo attacco contro le carte Bancomat è il fatto che per richiedere la generazione di un crittogramma (comando Generate Application Cryptogram) occorre prima inizializzare l'applicazione (comandi Select e Get Processing Options). A sua volta l'inizializzazione azzera lo stato della carta ed in particolare l'informazione che indica se è stato verificato il PIN o meno. Quindi con un attacco pre-play verso carte Bancomat verrebbero sì generati tanti crittogrammi per future transazioni ma questi conterrebbero tutti l'indicazione che non è stato verificato il PIN e quindi le relative transazioni verrebbero tutte rifiutate dal Centro Servizi.

Si può quindi concludere che l'attacco pre-play non costituisce una minaccia per le carte Bancomat.

B Test condotti dal Politecnico di Torino

Al fine di verificare le possibilità di attacchi concreti sulle carte a chip condotti da personale con buone conoscenze di sicurezza informatica e di elettronica, con l'uso di laboratori sperimentali di livello universitario, il Consorzio Bancomat ha fornito al Politecnico di Torino il seguente campione di carte anonime:

- carta A, con numero identificativo 6743090018006095279;
- carta B, con numero identificativo 00239503;
- carta C, con numero identificativo 2694 4223;
- carta D, con numero identificativo 2694 4222.

Su queste carte sono stati effettuati vari test ottenendo i seguenti risultati.

Estrazione del PIN tramite comandi software: non possibile.

La verifica è stata condotta inviando comandi corretti con parametri errati ed anche comandi inesistenti alle carte. I test hanno avuto una durata unitaria di 8 ore e sono stati ripetuti in vari giorni visto che includevano la generazione di dati casuali che quindi cambiano ad ogni svolgimento del test. In nessun caso le carte hanno mai mostrato comportamenti anomali ed in particolare – come previsto – non è mai stato possibile estrarre il PIN dalla carta.

Attacchi di power-analysis mirati alle chiavi crittografiche memorizzate nel chip: non possibili.

Usando le apparecchiature di laboratorio dei Dipartimenti di Automatica e Informatica (DAUIN) e di Elettronica e Telecomunicazioni (DET) è stata misurata la corrente assorbita dalle carte durante le operazioni crittografiche che coinvolgono quantità di sicurezza, ovvero la generazione dei seguenti crittogrammi:

- AAC (Application Authentication Cryptogram);
- ARQC (Authorisation Request Cryptogram);
- TC (Transaction Certificate).

Ciascun esperimento ha richiesto circa 6 ore perché è stata necessaria prima la registrazione di un migliaio di forme d'onda (a fronte dell'invio dello stesso comando) e poi la loro analisi differenziale per verificare se ci fossero elementi comuni dovuti all'uso della stessa chiave crittografica.

In nessun esperimento sono state evidenziate variazioni che possano portare a conoscere le chiavi crittografiche presenti all'interno del chip.

Si può quindi concludere che le prove sperimentali condotte dal Politecnico di Torino confermano le analisi scientifiche e documentali circa la non estraibilità del PIN e la non clonabilità delle carte a chip tramite procedure software o power analysis.

C Definizioni

ATM (Automatic Teller Machine) – terminale usato per il prelievo di contanti;

chip – dispositivo elettronico di ridotte dimensioni (circa 1 centimetro quadrato) in grado di svolgere funzioni di memoria e/o di calcolo;

CAM (Card Authentication Method) – metodo usato per verificare l'autenticità della carta quando introdotta in un PSO o ATM;

CVM (Cardholder Verification Method) – metodo usato per verificare se chi esibisce la carta è il titolare della stessa;

Centro Servizi – un centro di elaborazione dati che ha il compito di verificare ed autorizzare le transazioni richieste dalle carte di pagamento tramite i diversi terminali;

emettitore – ente che ha emesso la carta elettronica (es. la banca presso cui il cliente ha un conto corrente);

IAD (Issuer Application Data) – dati applicativi del protocollo EMV specifici di ciascun emettitore e trasmessi dalla carta al verificatore in modalità sicura;

issuer – si veda "emettitore";

MAC (Message Authentication Code) – codice crittografico che dimostra l'integrità e l'autenticità del messaggio o dei dati a cui è associato (integrità significa poter sapere se i dati del messaggio sono stati modificati dopo la loro creazione mentre l'autenticità dimostra chi è l'autore del messaggio);

microcircuito – termine italiano per la parola inglese "chip" (vedi);

owner – si veda "titolare";

PIN (Personal Identification Number) – numero associato univocamente ad una carta di pagamento, necessario per lo svolgimento di molte operazioni e consegnato in modo sicuro al titolare che ha il dovere di mantenerlo riservato;

POS (Point-Of-Sale) – terminale usato per il pagamento di un acquisto;

shim – apparecchiatura (solitamente miniaturizzata) inserita internamente o esternamente ad un terminale per registrare i dati scambiati tra terminale, carta e titolare;

terminale – apparecchiatura in cui viene inserita la carta elettronica, può essere un POS o un ATM;

titolare – la persona fisica a cui è stata consegnata la carta di pagamento ed il relativo PIN;

TVR (Terminal Verification Results) – il risultato delle verifiche svolte dal terminale e dalla carta trasmesso al Centro Servizi.

D Riferimenti bibliografici

[1] EMVco, "EMV Integrated Circuit Card Specifications for Payment Systems – Book 2, Security and Key Management", Versione 4.3, Novembre 2011

[2] MCU Engineering Co. Ltd, "IC crack", http://www.copy-mcu.com/pcb/ic-crack/

[3] Consorzio Bancomat, "IC CARD TECHNICAL SPECIFICATION", documento SPE/DEF/001, versione 1.5.0 (10/3/2011)

[4] P.Kocher, J.Jaffe, and B.Jun, "Introduction to Differential Power Analysis and Related Attacks", 1998
http://www.cryptography.com/public/pdf/DPATechInfo.pdf

[5] H.Pelletier and X.Charvet, "Improving the DPA attack using Wavelet transform", NIST Physical Security Testing Workshop, 2005
http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-3/physec/papers/physecpaper14.pdf

[6] S.J.Murdoch, S.Drimer, R.Anderson, and M.Bond, "Chip and PIN is Broken", Proc. of the 2010 IEEE Symposium on Security and Privacy, May 16-19, 2010, Oakland (CA, USA), pp. 433–446
http://www.cl.cam.ac.uk/~sjm217/papers/oakland10chipbroken.pdf

[7] S.J.Murdoch, S.Drimer, R.Anderson, and M.Bond, "EMV PIN verification 'wedge' vulnerability", February 2010
http://www.cl.cam.ac.uk/research/security/banking/nopin/

[8] http://www.smartcarddetective.com/

[9] http://code.google.com/p/smartcarddetective/

[10] http://www.smartarchitects.co.uk/opencart/index.php?route=product/category&path=35

[11] S.Sellami, "L'imparable escroquerie à la carte bancaire", Le Parisien, 24 January 2012, http://www.leparisien.fr/faits-divers/l-imparable-escroquerie-a-la-carte-bancaire-24-01-2012-1826971.php

[12] M.Bond, O.Choudary, S.J.Murdoch, S.Skorobogatov, R.Anderson, "Chip and Skim: cloning EMV cards with the pre-play attack", http://arxiv.org/abs/1209.2531